Policy Constraints Extension

References:
```
X.509 sections: 12.4.2, 12.4.2.3
RFC 2459 sections: 4.2, 4.2.1.12
FPKI Profile sections: 1.2.6.2, 1.2.7, 1.2.13,
 3.2.2.1.1
MISPC sections: 3.1.3.3
DII PKI Functional Specification sections: 3.2.2.3,
 3.2.4.1.2
```

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the certificate issuer enable the policyConstriants (PC) extension in CA certificates?		
Does the issuer not include the PC extension in EE certificates?		
Does the issuer always set either inhibitPolicyMapping and/or requireExplicitPolicy if it includes the PC extension in the certificate?		
Except for the Root-CA certificate, does every certificate issued include the policyConstraints extension with the requireExplicitPolicy field set with SkipCerts set to zero?		
If the requireExplicitPolicy field is present, does the issuer include in the certificatePolicies extension at least one of the policies applicable to the certificate?		
Does the issuer flag the extension as critical?		
Does the issuer not include this extension in the self-signed certificates?		
In processing a received certificate with the PC extension present, does the certificate user recognize it as a CA certificate?		
Upon encountering a null policy constraints field, is the certificate user able to handle this condition without failing, malfunctioning, or		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
The requireExplicitPolicy is present with a value of 0. Starting with the certificates issued by the subject CA and continuing until the certification path ends, does the certificate user check that the certificates policies extension of all certificates contain an acceptable policy identifier?		1
The requireExplicitPolicy is present with an integer value greater than 0. Starting with the certificates issued by the nominated CA and continuing until the certification path ends, does the certificate user check that the certificates policies extension of all certificates contain an acceptable policy identifier?		1, 2
The inhibitPolicyMapping is present with a value of 0. Does the certificate user not process policy mapping, starting with the certificates issued by the subject CA and continuing until the certification path ends?		
The inhibitPolicyMapping is present with an integer value greater than 0. Does the certificate user not process policy mapping, starting with the certificates issued by the nominated CA and continuing until the certification path ends?		2

Other information:

In processing a received certificate, if the certificate fails validation what does the implementation do?

1) An acceptable policy identifier is the identifier of the certificate policy required by the user of the certification path or the identifier of a policy that has been declared equivalent to it through policy mapping

2) The nominated CA is a CA that is the subject of a subsequent certificate in the certification path (as indicated by the integer value).